AFRL-AFOSR-UK-TR-2015-0026

Dynamic Information Management and Exchange for Command and Control Applications

Maribel Fernandez

KING'S COLLEGE LONDON
THE STRAND
LONDON WC2R 2LS UNITED KINGDOM

EOARD GRANT #FA8655-10-1-3047

Report Date: March 2015

Final Report from 24 August 2010 to 28 February 2015

Distribution Statement A: Approved for public release distribution is unlimited.

Air Force Research Laboratory
Air Force Office of Scientific Research
European Office of Aerospace Research and Development
Unit 4515, APO AE 09421-4515

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
01 March 2015	Final Report	24 August 2010 – 28 February 2015

4. TITLE AND SUBTITLE

Dynamic Information Management and Exchange for Command and Control Applications

5a. CONTRACT NUMBER

5b. GRANT NUMBER

FA8655-10-1-3047

5c. PROGRAM ELEMENT NUMBER

61102F

6. AUTHOR(S)

Prof Maribel Fernandez

5d. PROJECT NUMBER

5d. TASK NUMBER

5e. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

KING'S COLLEGE LONDON
THE STRAND
LONDON WC2R 2LS UNITED KINGDOM

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

EOARD
Unit 4515
APO AE 09421-4515

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/AFOSR/IOE (EOARD)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

AFRL-AFOSR-UK-TR-2015-0026

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution A: Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The main goal of this project was to develop a new model of access control to facilitate the specification of policies in highly dynamic scenarios. The requirement was to have a mathematically well dened model so that properties of policies can be proven, and so that verifiably correct systems can be developed. We have achieved this general goal: we have developed an expressive category-based metamodel of access control, which has a rewrite-based semantics allowing us to prove correctness properties of policies. Previously dened access control models are instances of our metamodel and in addition the metamodel encompasses distributed models, as well as federative policies (where a global access control policy governing the federation is dened as a composition of local policies specified by individual members of the federation).

15. SUBJECT TERMS

EOARD, Information Management, Distributed Computing, Information Assurance

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18, NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			James H Lawton, PhD
UNCLAS	UNCLAS	UNCLAS	SAR	8	19b. TELEPHONE NUMBER *(Include area code)* (703) 696-5999

Extension to the project on "Dynamic Information Management and Exchange for Command and Control Applications"

Modelling and Enforcing Category-Based Access Control via Term Rewriting

FA8655-10-1-3047

Maribel Fernandez (PI)
Anatoli Degtyarev (Co-Investigator)

King's College London

Final report submitted to the European Office of Aerospace Research & Development

March 2015

Distribution A: Approved for public release; distribution is unlimited.

Abstract

The main goal of this project was to develop a new model of access control to facilitate the specification of policies in highly dynamic scenarios. The requirement was to have a mathematically well defined model so that properties of policies can be proven, and so that veriafiably correct systems can be developed.

We have achieved this general goal: we have developed an expressive category-based metamodel of access control, which has a rewrite-based semantics allowing us to prove correctness properties of policies. Previously defined access control models are instances of our metamodel and in addition the metamodel encompasses distributed models, as well as federative policies (where a global access control policy governing the federation is defined as a composition of local policies specified by individual members of the federation).

Using the rewrite-based operational semantics of the metamodel, we have defined a policy composition framework: operators to combine policies can be defined using rules, and properties of the resulting global policy can be proven in terms of the properties of the individual policies in the combination. We have also given a set of core axioms to specify emergency policies in the category based metamodel.

In addition, an extension of the category based access control metamodel has been proposed to include obligations. The extended metamodel allows security administrators to check whether a policy combining authorisations and obligations is consistent. This is particularly important in the context of emergency management.

We have defined a graphical representation of category-based policies, and shown how answers to usual administrator queries can be automatically computed, and properties of access control policies can be checked.

The results obtained in the project have been presented in international conferences and published in peer-reviewed conference proceedings and in international journals.

We are grateful for the financial support provided by AFOSR and EOARD in relation to Grant FA8655-10-1-3047. We thank Dr James Lawton for his always excellent support and advice.

Distribution A: Approved for public release; distribution is unlimited.

1 Introduction

Access control policies specify which actions users are authorised to perform on protected resources. An authorisation may entail an obligation to perform another action on the same or another resource. Standard languages for the specification of access control policies include also a number of primitives to specify obligations associated with authorisations. For example, within XACML, an obligation is a directive from the Policy Decision Point (PDP) to the Policy Enforcement Point (PEP) specifying an action that must be carried out before or after an access is approved. If the PEP is unable to comply with the directive, the access might not be realised, even if it is authorised. Given the complexities involved in the definition of access control and obligation policies for command and control applications, formal methods to analyse and reason about policies are essential. This is particularly important in the case of systems dealing with access control in the context of emergency situations, where users' rights and obligations may need to change in order to cope with specific emergencies.

In this project we have addressed these issues by developing a category-based metamodel for access control, which identifies a core set of principles of access control, abstracting away many of the complexities that are found in specific access control models in order to simplify the tasks of policy writing and policy analysis. A key aspect of the metamodel is to focus attention on the notion of a *category*. A category is a class of entities which share some property. Classic types of groupings used in access control, like a role, a security clearance, a discrete measure of trust, etc., are particular instances of the more general notion of category. In category-based access control (CBAC) policies, permissions are assigned to categories of users, rather than to individual users. Categories can be defined on the basis of e.g., user attributes, geographical constraints, resource attributes. In this way, permissions can change in an autonomous way (e.g., when a user attribute changes), unlike, e.g., role-based access control models, which require the intervention of a security administrator. The category-based metamodel does not make any specific assumptions on the components of the system. It is an abstract model of access control and obligations that can be instantiated in various ways to satisfy specific requirements.

The category-based metamodel for access control has been equiped with a rewriting semantics, which allows us to study implementations (rewriting provides an operational semantics for polices) and to prove properties of the policies. It is expressive: we have shown that all the access control models that are currently in use can be specified as instances of the metamodel. To accomodate obligations, the metamodel has been extended and examples of policies have been developed in the context of emergency management.

In critical domains, such as policies for command and control, it is highly desirable that access control models and policies be mathematically well defined so that properties of policies can be verified. Formal methods to analyse and reason about policies are essential for systems dealing with access control in the context of emergency situations, where users' rights may need to change in order to cope with specific emergencies. The rewrite-based operational semantics for the category-based metamodel allows us to use standard rewriting tools (such as CiME, Maude, Aprove, TTT, etc.) to verify security policies, e.g., to ensure that each access request has a unique answer (the latter is proved by checking the confluence and termination of the rewrite relation, which the above mentioned tools do).

Distribution A: Approved for public release; distribution is unlimited.

2 Main Results

The main results obtained in this project are:

1. We defined the *distributed category-based access control metamodel*, and provided a *rewrite-based operational semantics*, which can be used to model single access control policies or distributed (federative) policies defined as a combination of local policies. The access control metamodel was presented in [3]. The extension to deal with distributed policies is presented in [4], where a declarative, rewrite-based operational semantics is given. Distributed systems are seen as federations in which each component preserves its autonomy: the metamodel provides mechanisms to define *combinations* of policies, by defining general policy-combining operators, with a formal operational semantics for *access request evaluation* in centralised as well as in distributed contexts where information is shared. The metamodel includes mechanisms for the resolution of conflicts between local and global policies.

2. We have incorporated the notion of *obligation* in the metamodel. To specify dynamic policies involving authorisations and obligations in the metamodel, we adjusted the notion of an *event* used in previous work, and described a set of core axioms for defining *obligations*. In addition, we provide a rewrite-based operational semantics for the extended metamodel, which can be used to specify policies and derive implementations. The rewrite-based semantics specifies how *authorisations and obligations* are evaluated, and includes mechanisms for the resolution of conflicts between authorisations and obligations. These results are published in [1].

3. Based on the metamodel, we have defined a graphical framework for the analysis of policies that aims at easing the specification and verification tasks for security administrators. Using a visual representation of policies, we show how answers to usual administrator queries can be automatically computed, and properties of access control policies (such as, every access request receives a unique answer) can be checked. For example, the fact that the policy ensures a "separation of duty" constraint (where no user should be allowed to perform two conflicting actions on the same resource), can be easily proved using graph-based algorithms and rewriting techniques. We show applications of the framework to the analysis of policies in distributed environments, and in particular policies that include management of rights in emergency situations. These results are published in [2].

In addition, the following results have been implemented by students at King's College London, as part of their final year projects (supervised by M. Fernández).

1. Distributed category based access control (item 1 above): this has been applied in three individual UG projects, where students implemented access control policies for a bank, a hotel and a hospital.

2. Event handler for emergency policies (item 2 above): this has been implemented in two UG projects, one project developed a category-based access control system for a hospital, the other focused on the infrastructure required for the event processing (dealing with mechanisms to obtain and process data that trigger the application of emergency policies).

Distribution A: Approved for public release; distribution is unlimited.

3. Policy Manager: a graphical environment for the analysis of policies (item 3 above) was implemented in Ruby as part of an UG project.

3 Publications

For more details on the work described in this report, we refer to the annual reports (submitted in August 2011, 2012, 2013, 2014) and to the following publications[1] (attached).

- Clara Bertolissi, Maribel Fernández. A metamodel of access control for distributed environments: Applications and properties. Information and Computation 238: 187-207 (2014). Elsevier.
- S. Alves, A. Degtyarev, M. Fernández. Access control and obligations in the category-based metamodel: a rewrite-based semantics. Proceedings of LOPSTR 2014, Logic-Based Program Synthesis and Transformation - 24th International Symposium, Canterbury, UK. September 2014. Proietti, Maurizio, Seki, Hirohisa (Eds.), Lecture Notes in Computer Science, Vol. 8981. Springer, 2015.
- S. Alves, M. Fernández. A Framework for the Analysis of Access Control Policies with Emergency Management. Proceedings of LSFA 2014, 9th Workshop on Logical and Semantic Frameworks, with Applications, Brasilia, Brazil, September 2014. Electronic Notes in Theoretical Computer Science (to appear).

4 Conclusions and future work

The access control metamodel developed in this project is expressive enough to deal with most of the features relevant to authorisations and obligations and provides means to reason about them. We consider that the project has achieved all its aims, however, some important issues need to be further developed: the typing relation for events (e.g., to identify events that trigger emergency policies), the definition of mechanisms to deal with accountability in case of failed obligations, and various types of administrative updates on policies (e.g., delegation of rights). These are topics for future research.

We also wish to provide more mechanisms for analysing dynamic properties of policies and helping administrators to develop and manage policy updates. With this aim in view, we plan to develop a version of the Policy Manager tool within PORGY, an environment we are developing to provide visualisation and simulation features for systems specified via port-graph rewriting.

Acknowledgements

The late Dr Steve Barker worked in this project during 2010 and 2011; his inspirational ideas provided the basis for this project. Steve will always be remembered.

[1] Authors are listed in alphabetically order, as usual for theoretical computer science papers.

Distribution A: Approved for public release; distribution is unlimited.

We are grateful for the support provided by the European Office of Aerospace Research & Development in relation to Grant FA8655-10-1-3047. We thank Dr James Lawton for his always excellent support and advice.

References

[1] Sandra Alves, Anatoli Degtyarev, and Maribel Fernández. Access control and obligations in the category-based metamodel: a rewrite-based semantics. In *Proceedings of LOPSTR 2014, Logic-Based Program Synthesis and Transformation - 24th International Symposium, Canterbury, UK. September 2014. Selected Papers.*, Lecture Notes in Computer Science. Springer, 2015.

[2] Sandra Alves and Maribel Fernández. A framework for the analysis of access control policies with emergency management. *Electronic Notes in Theoretical Computer Science, Special Issue: Proceedings of LSFA 2014, 9th Workshop on Logical and Semantic Frameworks, with Applications, Brasilia, Brazil, September 2014*, 2015.

[3] S. Barker. The next 700 access control models or a unifying meta-model? In *SACMAT 2009, 14th ACM Symposium on Access Control Models and Technologies, Stresa, Italy, June 3-5, 2009, Proceedings*, pages 187–196. ACM Press, 2009.

[4] Clara Bertolissi and Maribel Fernández. A metamodel of access control for distributed environments: Applications and properties. *Inf. Comput.*, 238:187–207, 2014.

Distribution A: Approved for public release; distribution is unlimited.